

# How to Enable "Geeks on Tap - Security Assessment Tool" in Google Workspace

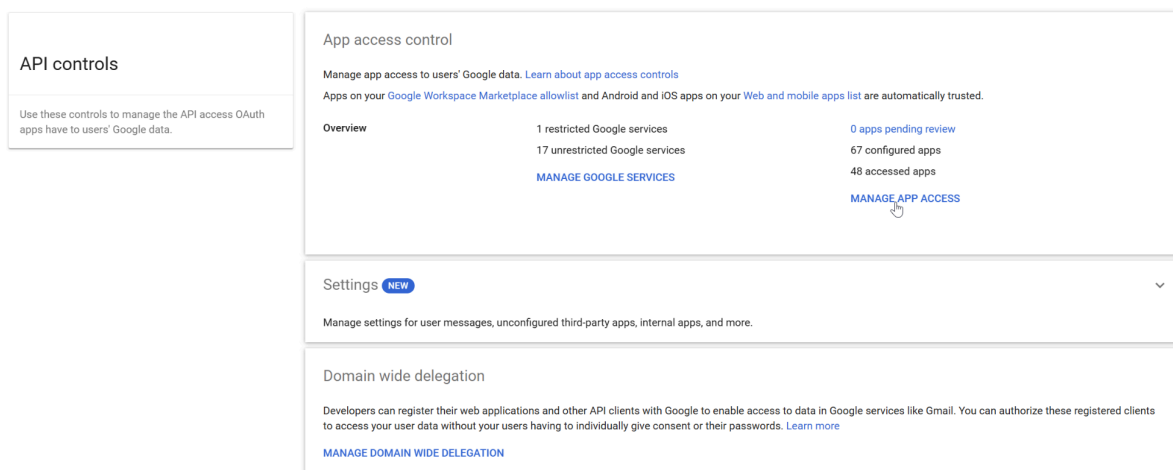
## Instructions for Google Workspace Admins

There are two primary ways to trust an application. The most direct method is using the **App Access Control** settings. Please follow the steps below.

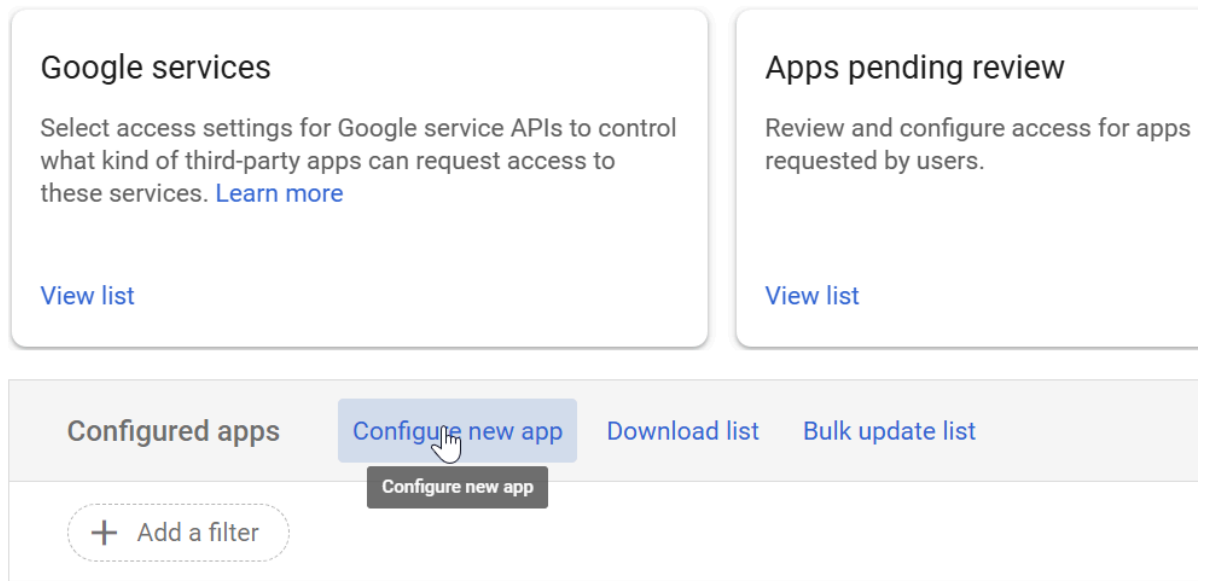
### Method 1: Trusting the App via App Access Control (Recommended)

This method uses the app's unique **Client ID** to find and trust it, applying the change to your entire organization or specific groups/organisational units (OUs).

1. Log in to your **Google Admin console** (at [admin.google.com](https://admin.google.com)).
2. In the left-hand menu, navigate to **Security > Access and data control > API controls**.
3. In the "App access control" card, click **Manage App Access**.



4. You will see a list of "Accessed" apps. Click the "**Configure new app**" dropdown.



5. In the search box, paste our app's **Client ID**:  
`272019090134-fs2kd055tc18vt69dk5umgk8nhda481a.apps.googleusercontent.com`
6. Our application, **Geeks on Tap - Security Assessment Tool**, will appear in the search results. Click **Select**.
7. On the next screen, check the box for our **Client ID**.
8. Select the scope of this change:
  - To trust it for **everyone**, leave the top-level Organisational Unit selected.
  - To trust it for **specific users**, select the Organisational Unit(s) or Group(s) that need access.
9. Click **Continue**.

10. On the "Access to Google data" screen, choose the **"Trusted: Can access all Google services"** option.

Selected application

Geeks on Tap - Security Assessment Tool Web Verified

Access to Google Data

Choose an access type to specify which data this app can request from users signing in with their Google Account.  
[Learn more about app access to Google data](#)

☒ Trusted

This app can request access to user data in any Google service via OAuth 2.0 scopes.  
[What to expect with trusted access](#)

☐ Exempt from having API access blocked by Context-Aware Access levels.  
Applies only if this app was added by OAuth client ID. [Learn about exempting apps.](#)  
This exception is enforced only if a Context-Aware Access level in the same org unit selected in Scope also allows exemptions.  

Allowlisting an app here doesn't mean it's immediately exempted from API access blocks. You'll need to explicitly exempt the app during access level assignments to enforce the exemption. [Learn more](#)

☐ Limited

This app can request access to user data in any Google service marked unrestricted under Google services.  
[What to expect with limited access](#)

☐ Specific Google data

This app can only request access to user data from the Google services specified below. Note, you must include the Google Sign-in scope below to allow users to sign in with their Google Account.

Drive 1 scope

Google Workspace Admin 8 scopes

Google Sign-in 3 scopes

[Update Google services or scopes](#)

[Back](#) [Cancel](#) [Continue](#)

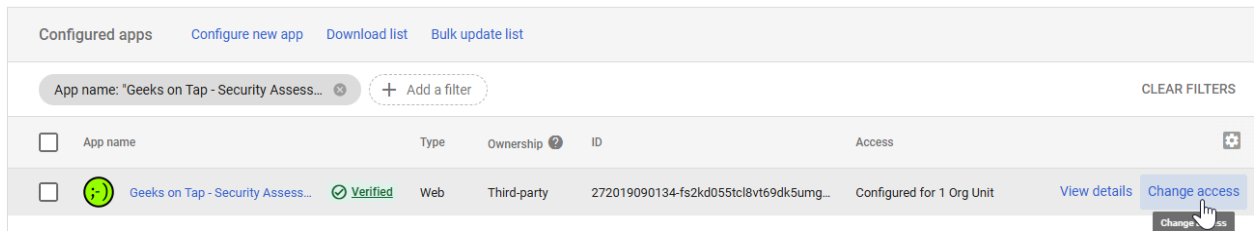
11. Click **Continue**, review your settings, and then click **Finish**.

## Method 2: Reviewing a Blocked or Limited App

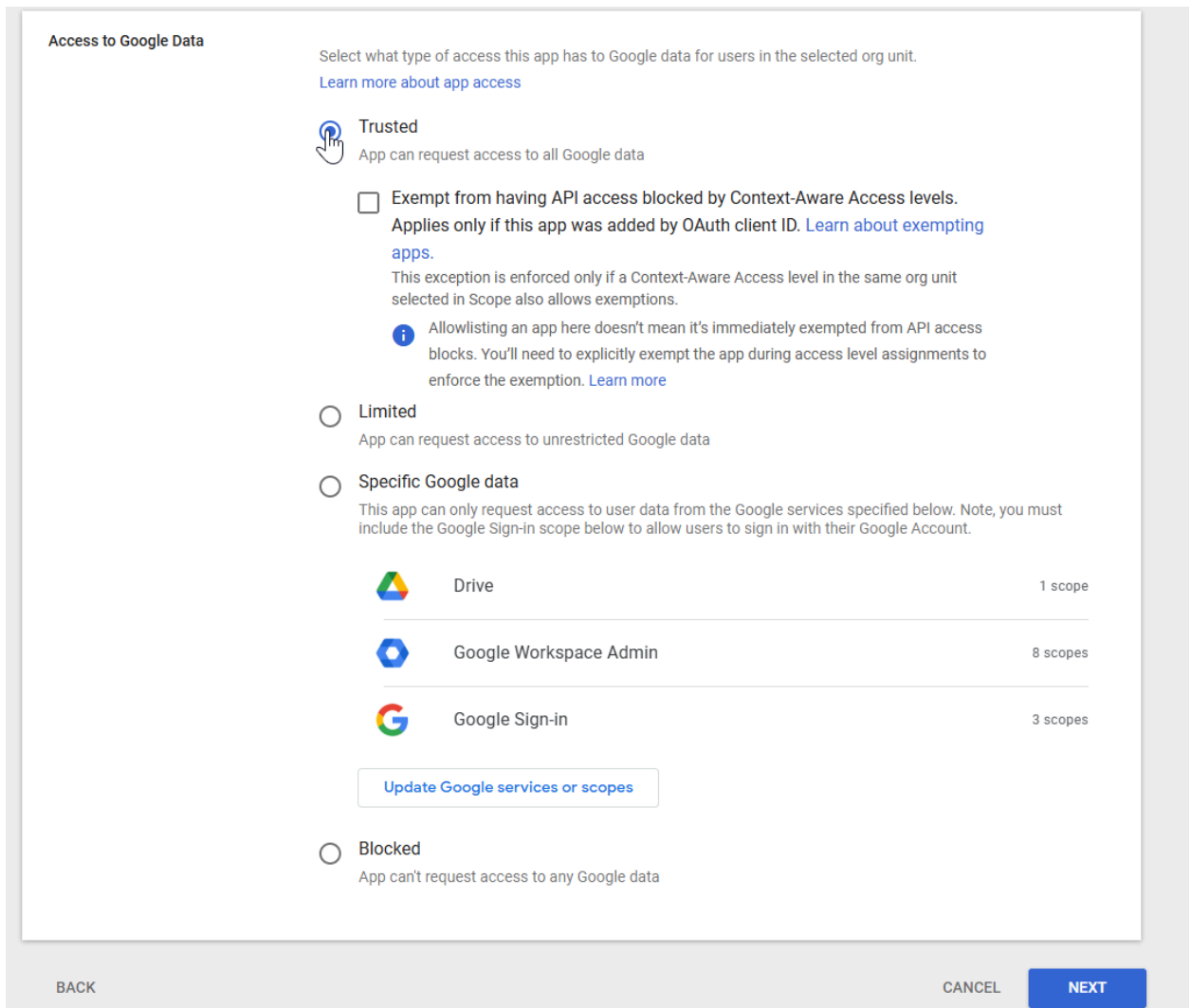
If a user has already tried to install the app and was blocked, it may appear in your "Accessed" apps list with a "Blocked" or "Limited" status.

- Follow steps 1-3 from Method 1 to navigate to the **Manage Third-Party App Access** page.
- Look for **Geeks on Tap - Security Assessment Tool** in the list of apps. You can use the "Add a filter" option to search by app name.
- Click on the app name in the list.

4. In the app's detail panel, click the **"Change access"** link.



5. Select the OUs or Groups you wish to grant access to (or leave as-is for the whole organization).
6. Change the access level from "Blocked" or "Limited" to **"Trusted"**.



7. Click **Save**.

## Troubleshooting & Contact

If you have any questions about our application's security or the permissions it requires, please do not hesitate to contact our team.